(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 197 47 603 A 1**

(51) Int. Cl.[6]:
H 04 M 11/00
H 04 L 9/30
H 04 Q 7/32

(21) Aktenzeichen: 197 47 603.1
(22) Anmeldetag: 28. 10. 97
(43) Offenlegungstag: 20. 5. 99

(71) Anmelder:
Brokat Informationssysteme GmbH, 71034 Böblingen, DE

(74) Vertreter:
Gleiss & Große, Patentanwaltskanzlei, 70469 Stuttgart

(72) Erfinder:
Röver, Stefan, 71088 Holzgerlingen, DE; Groffmann, Hans-Dieter, Dr., 72145 Hirrlingen, DE

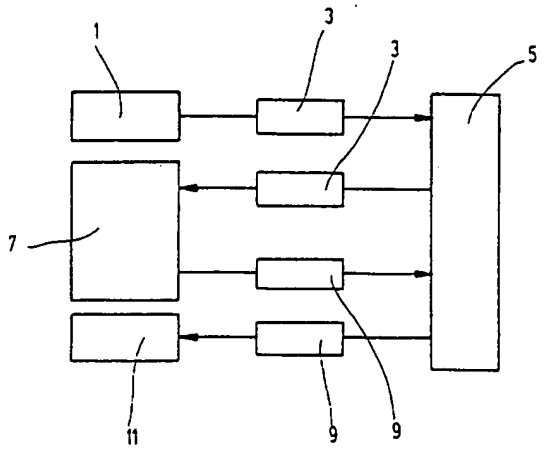
(56) Entgegenhaltungen:
DE 1 96 09 232 A1
DE 44 06 590 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum digitalen Signieren einer Nachricht

(57) Die Erfindung betrifft ein Verfahren zum digitalen Signieren einer Nachricht sowie die dazu notwendigen Mittel.



DE 197 47 603 A 1

DE 197 47 603 A 1

Im Zusammenhang mit der vorliegenden Erfindung wird unter einem digitalen Signieren einer Nachricht ein Vorgang verstanden, bei dem auf elektronischem Wege der Wille zur Abgabe und der Inhalt einer Nachricht bestätigt wird. Dies geschieht durch partielle oder vollständige Verschlüsselung der zu signierenden Nachricht oder durch Verschlüsselung einer kryptographischen Prüfsumme dieser Nachricht in eine signierte Nachricht mittels eines geheimen Schlüssels unter Anwendung eines mathematischen Verfahrens. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer signierten Nachricht entweder die signierte Nachricht als ganze oder die Signatur selbst verstanden. Die Signierung dient dazu, später eine Authentifizierung des Nutzers durchführen zu können. Im Zusammenhang mit der vorliegenden Erfindung wird also unter einer signierten Nachricht auch nur die elektronisch erzeugte Signatur der Nachricht verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer Nachricht jegliche Art von in elektronischer Form wiedergebbarer Information, beispielweise Zahlen, Buchstaben, Zahlenkombinationen, Buchstabenkombinationen, Grafiken, Tabellen etc. verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einem Signiergerät eine Einheit verstanden, die eine Signierung einer Nachricht durchführen kann, das heißt einen geheimen Schlüssel, ein mathematisches Verschlüsselungsverfahren, Dialogmöglichkeiten mit dem Signierer oder Nutzer, gegebenenfalls notwendigen Schnittstellen und eine Sende- und Empfangsvorrichtung aufweist. Diese Einheit kann aus verschiedenen Elementen, zum Beispiel aus einer Chip-Karte und einem Lesegerät oder einer Chip-Karte und einem Mobilfunktelefon, aufgebaut sein. Eine Signiervorrichtung ist im Zusammenhang mit der vorliegenden Erfindung eine Komponente des Signiergeräts, die den geheimen Schlüssel und/oder das Verschlüsselungsverfahren und/oder eine Schnittstelle zu beiden oder einer der vorgenannten Komponenten aufweist.

Aufgrund der erfindungsgemäß besonders bevorzugten Verwendung des Funktelefonnetzes zur Übertragung der zu signierenden Nachrichten an ein Signiergerät, das in vorteilhafter Ausgestaltung als Mobilfunktelefon ausgeführt ist, ist es möglich, von einem handelsüblichen Rechner mit Anschluß an einen entsprechenden Nachrichten-Server, zum Beispiel via e-Mail, Nachrichten an das Signiergerät zu übermitteln, ohne am Rechner selbst Installationen oder andere Veränderungen vornehmen zu müssen.

In besonders bevorzugter Ausführungsform sieht die Erfindung ein Verfahren der vorgenannten Art vor, wobei die zu signierende Nachricht von einer auch als Nachrichtenquelle zu bezeichnenden Sendevorrichtung, beispielsweise einem PC, an eine Empfangsvorrichtung, beispielsweise einen Nachrichten-Server, übertragen wird, anschließend diese Nachricht von der Empfangsvorrichtung an ein der Sendevorrichtung zugeordnetes Signiergerät, insbesondere Mobilfunktelefon übertragen wird, anschließend diese Nachricht im Mobilfunktelefon signiert wird, und sodann an die Empfangsvorrichtung als Signatur, das heißt als signierte Nachricht, zurückübertragen wird.

Die Erfindung sieht also vor, daß von einer Nachrichtenquelle eine unsignierte bzw. zu signierende Nachricht an eine Empfangsvorrichtung, zum Beispiel einen Nachrichten-Server, übertragen wird. Die Empfangsvorrichtung nimmt dann eine Zuordnung der zu signierenden Nachricht zu dem Signiergerät, insbesondere dem Mobiltelefon, vor. Dies geschieht entweder durch eine in der Empfangsvorrichtung hinterlegte Dokumentation oder über Informationen, die zusammen mit der zu signierenden Nachricht von der Sendevorrichtung an die Empfangsvorrichtung übertragen wurde. Die Zuordnung des Signiergeräts, vorteilhafterweise des Mobilfunktelefons, zu der Nachrichtenquelle braucht also keine räumliche Zuordnung zu sein, sondern ist eine rein informatorische Zuordnung. Die Zuordnung besteht also darin, festzustellen, welches Signiergerät und damit welcher Nutzer die empfangene, zu signierende Nachricht signieren soll. Das in bevorzugter Ausführungsform der Erfindung eingesetzte Mobilfunktelefon ist in vorteilhafter Weise in der Lage, eine zu signierende Nachricht darzustellen und auf Anweisung des Nutzers und unter Zuhilfenahme der in vorteilhafter Weise eingesetzten Chip-Karte zu signieren. Die auf diese Weise signierte Nachricht wird der Empfangsvorrichtung übermittelt und dort gegebenenfalls mit der ursprünglichen Nachricht verglichen und authentifiziert. Von der Empfangsvorrichtung wird die signierte und gegebenenfalls authentifizierte Nachricht dann an einen Adressaten weitervermittelt.

Die Erfindung betrifft auch ein vorgenanntes Verfahren, wobei in vorteilhafter Weise vorgesehen ist, zum Signieren ein Public-Key-Verfahren einzusetzen, bei dem die Sendevorrichtung über einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt. Diese Vorgehensweise bietet den Vorteil, daß die Schlüssel nicht übermittelt werden müssen.

In einer weiteren vorteilhaften Ausgestaltung betrifft die Erfindung ein vorgenanntes Verfahren, wobei die zu signierende Nachricht oder die bereits signierte Nachricht, das heißt zum Beispiel die Signatur zwischen Empfangsvorrichtung und Signiergerät, insbesondere Mobilfunktelefon, mittels des Short-Message-Service (SMS) übertragen werden. In besonders bevorzugter Ausführungsform kann vorgesehen sein, daß sowohl die Übertragung der zu signierenden Nachricht von der Empfangsvorrichtung zum Mobilfunktelefon als auch die Übertragung der signierten Nachricht bzw. der Signatur vom Mobilfunktelefon zur Empfangsvorrichtung mittels des SMS durchgeführt wird.

Die Erfindung sieht in einer weiteren Ausführungsform vor, daß die zu signierende Nachricht mittels einer im Mobilfunktelefon vorgesehenen Anzeigeeinrichtung dargestellt wird. Dies kann auf dem Display handelsüblicher Mobilfunktelefone geschehen. Auf diese Weise lassen sich ohne weiteres einfache Texte, wie zum Beispiel Banktransaktionen oder sogar einfache Grafiken, darstellen.

Im Anschluß an diese gegebenenfalls vorgesehene Darstellung gibt der Benutzer in einem dafür vorgesehenen Dialog eine entsprechende Anweisung zur Auslösung des Signierens. In besonders bevorzugter Ausführungsform sieht die Erfindung ein Verfahren der vorgenannten Art vor, wobei der zum Signieren notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons abgelegt ist und dieser Schlüssel mittels einer über eine Tastatur des Mobilfunktelefons eingebbaren Geheimzahl (im folgenden PIN genannt) freigegeben wird. In vorteilhafter Weise kann durch eine entsprechende übliche Programmierung des Mobilfunktelefons sichergestellt werden, daß die eingegebene PIN nur auf die Chip-Karte übertragen wird und nicht von außen abgehört werden kann.

In einer weiteren alternativen Ausgestaltung der vorgenannten erfindungsgemäßen Verfahren ist vorgesehen, daß der zum Signieren notwendige geheime Schlüssel über eine Tastatur des Mobilfunktelefons eingegeben wird.

In einer weiteren bevorzugten Ausführungsform der Erfindung ist vorgesehen, daß in einem der vorgenannten Verfahren der geheime Schlüssel nicht nur auf der Chip-Karte des Mobilfunktelefons gespeichert ist, sondern dort auch das Signieren der Nachricht durchgeführt wird. Damit kann in vorteilhafter Weise sichergestellt werden, daß der geheime Schlüssel auf keinen Fall die Chip-Karte verläßt und

tung **27** trägt dafür Sorge, daß die Befehle oder Kommandos der Signiervorrichtung **21** ausgeführt werden und die signierte Nachricht **9** über die Signiervorrichtung **21** an die Sende- und Empfangseinrichtung **15** weitergegeben wird. Das heißt, die Chip-Karten-Einrichtung **27** stellt eine Schnittstelle zwischen Signiervorrichtung **21** und der Chip-Karte **25** dar.

Die **Fig. 3** stellt in sehr vereinfachter schematischer Darstellung eine erfindungsgemäße Chip-Karte **25** dar. Diese umfaßt im wesentlichen ein Kontaktierpad **31** sowie eine Speichereinheit **27** und ein Kryptographiemodul **29**. In der Speichereinheit **27** ist der für die Erstellung der signierten Nachricht **9** notwendige geheime Schlüssel abgelegt. Das Kryptographiemodul **29** dient der Verschlüsselung der zu signierenden Nachricht **3**, beispielsweise mittels eines RSA-Verfahrens. Über das Kontaktierpad **31** kann die Speichereinheit **27** bzw. das Kryptographiemodul **29** mit der Chip-Karten-Einrichtung **27** in kommunikativer Verbindung stehen. Aus Gründen der Übersichtlichkeit sind weitere, für den Betrieb der Chip-Karte **25** notwendige Elemente wie beispielsweise ein Controller in der Darstellung der **Fig. 3** nicht dargestellt.

Patentansprüche

1. Verfahren zum digitalen Signieren einer über ein Kommunikationsnetzwerk an ein Signiergerät übertragenen und zu signierenden Nachricht, wobei die zu signierende Nachricht mittels eines Telefonnetzes an das Signiergerät übertragen wird.
2. Verfahren nach Anspruch 1, wobei das Signiergerät ein Mobilfunktelefon ist.
3. Verfahren nach einem der vorhergehenden Ansprüche, wobei die zu signierende Nachricht von einer Sendevorrichtung an eine Empfangsvorrichtung, diese Nachricht anschließend von der Empfangsvorrichtung über ein Telefonnetz, insbesondere ein Mobilfunktelefonnetz, an ein der Sendevorrichtung zugeordnetes Mobilfunktelefon übertragen wird, diese Nachricht sodann im Mobilfunktelefon signiert und an die Empfangsvorrichtung als signierte Nachricht zurückübertragen wird.
4. Verfahren nach einem der vorhergehenden Ansprüche, wobei zur Signierung ein Public-Key-Verfahren eingesetzt wird, insbesondere ein Public-Key-Verfahren, bei dem die Sendevorrichtung über einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt.
5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachrichten zwischen Empfangsvorrichtung und Mobilfunktelefon mittels des Short-Message-Service (SMS) übertragen werden.
6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachricht vor der Signierung mittels einer im Mobilfunktelefon vorgesehenen Anzeigeeinrichtung dargestellt wird.
7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel über eine Tastatureinrichtung des Mobilfunktelefons eingegeben wird.
8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons abgelegt ist, und dieser Schlüssel mittels einer über eine Tastatureinrichtung des Mobilfunktelefons eingebbaren Geheimzahl (PIN) freigegeben wird.
9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Chip-Karte die Erstellung der signierten Nachricht durchführt.
10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon die Erstellung der signierten Nachricht durchführt und wobei der geheime Schlüssel aus der Chip-Karte gelesen wird.
11. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon zusätzlich als Sender zur Übermittlung der signierten Nachricht an die Empfangsvorrichtung dient.
12. Mobilfunktelefon mit einer Tastatur, einer Anzeigevorrichtung und einer Chip-Karten-Einrichtung zum Lesen und/oder Schreiben einer in das Mobilfunktelefon einsteckbaren Chip-Karte, gekennzeichnet durch eine Signiervorrichtung (**21**), insbesondere zur Erstellung einer signierten Nachricht (**9**) aus einer zu signierenden Nachricht (**3**) oder/und zur Kommunikation mit einer eine Signiervorrichtung (**21**) aufweisenden Chip-Karte (**25**).
13. Mobilfunktelefon nach Anspruch 12, dadurch gekennzeichnet, daß die Signiervorrichtung (**21**) mit der Tastatureinrichtung (**19**) zur Eingabe eines geheimen Schlüssels oder einer Geheimzahl verbunden ist.
14. Chip-Karte für ein Mobilfunktelefon, insbesondere nach einem der Ansprüche 12 oder 13, dadurch gekennzeichnet, daß die Chip-Karte (**25**) eine Signiervorrichtung (**21**) umfaßt, die eine Speichereinheit (**27**) zur Speicherung des für die Erstellung der signierten Nachricht (**9**) notwendigen geheimen Schlüssels aufweist.
15. Chip-Karte nach Anspruch 14, dadurch gekennzeichnet, daß die Chip-Karte (**25**) eine Signiervorrichtung (**21**) umfaßt, die aus einer vom Mobilfunktelefon (**7**) empfangenen zu signierenden Nachricht (**3**) eine signierte Nachricht (**9**) erstellt.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 197 47 603 A1
Int. Cl.[6]: H 04 M 11/00
Offenlegungstag: 20. Mai 1999

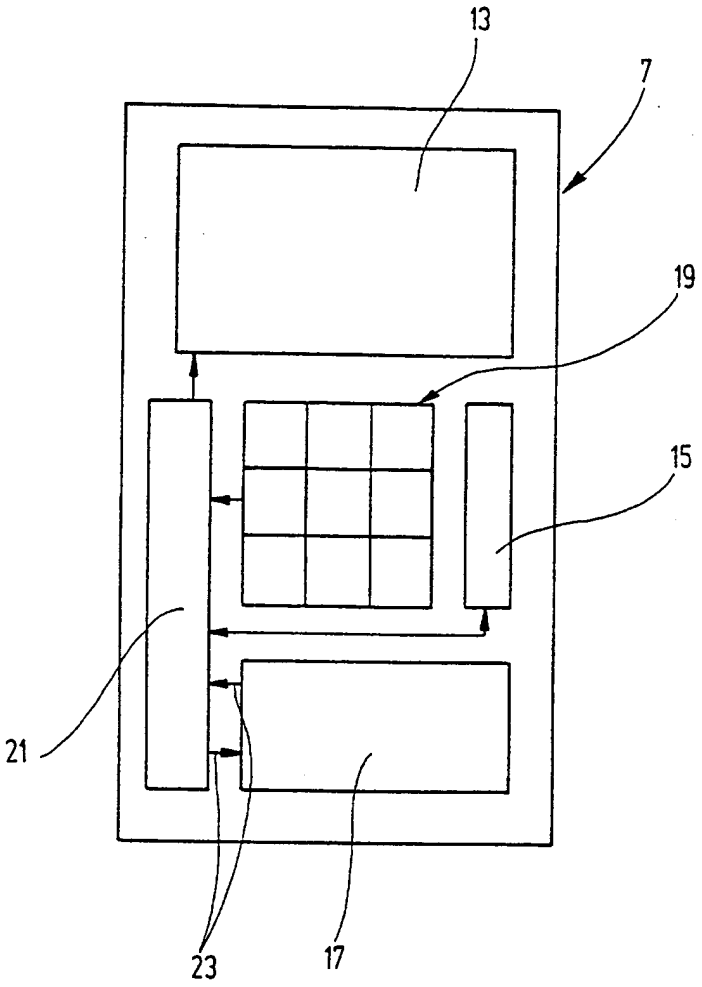


Fig. 2

197 47 603.1-31
Applicant: Brokat ...
Our File: NP-5893

Translation
of Patent Claims 1 to 8 Filed 21 September 2000

Claims

1. A method of digitally signing a communication which is transmitted through a communication network to a signing device and has to be signed, wherein the communication to be signed is first emitted by an emitting device, especially a PC, to a receiving device, said communication is subsequently transmitted by the receiving device via a telephone network, especially a mobile telephony network, to a signing device that is associated with the emitting device and designed as a mobile telephone, said communication is then signed in the mobile telephone on instruction of the user and thus the desire to emit as well as the contents of the communication are confirmed, said communication is, as a signed communication, retransmitted to the receiving device or to another receiver, and is then routed to an addressee.

2. The method according to claim 1, wherein a public key method is used for the signing, especially a public key method in which the signing device holds a secret key assigned to it and especially the receiving device holds the corresponding public key associated with the secret key, so that, if desired, the signed communication transmitted to the receiving device can there be compared to the original communication and be authenticated.

3. The method according to one of the preceding claims, wherein the communications between receiving device and mobile telephone are transmitted by way of short-message service (SMS).

4. The method according to one of the preceding claims, wherein the communication is displayed by a display means provided in the mobile telephone before it is signed.

5. The method according to one of the preceding claims, wherein the secret key required for the signing is input through a keypad of the mobile telephone.

6. The method according to one of the preceding claims, wherein the secret key required for the signing is stored in a chip card of the mobile telephone and said key is enabled by means of a secret number (PIN) to be input via a keypad of the mobile telephone.

7. The method according to one of the preceding claims, wherein the chip card performs the signing of the communication to be signed.

8. The method according to one of the preceding claims, wherein the mobile telephone performs the signing of the communication to be signed and wherein the secret key is read from the chip card.